International Journal of Information Systems Management Research and Development (IJISMRD)
ISSN(P): 2250-236X; ISSN(E): 2319-4480
Vol. 4, Issue 2, Apr 2014, 17-26
© TJPRC Pvt. Ltd.

TRANS STELLAR
• Journal Publications • Research Consultancy

THE ROLE OF DIGITAL CERTIFICATES IN CONTEMPORARY GOVERNMENT SYSTEMS: THE CASE OF UAE IDENTITY AUTHORITY

ALI M. AL-KHOURI
Emirates Identity Authority, Abu Dhabi, United Arab Emirates

ABSTRACT

Digital certificates provide advanced instruments for confirming identities in electronic environments. The application of digital certificates has been gaining global acceptance both in public and private sectors. In fact, the government field has witnessed increasing adoption of cryptographic technologies to address identity management requirements in cyberspace. The purpose of this article is to provide an overview of various governmental scenarios on the usage and application of digital certificates in the United Arab Emirates. The UAE government integrated public key infrastructure (PKI) technology into its identity management infrastructure since 2003. The article also explores the UAE digital identity issuing authority's position regarding government-to-government transactions and the prospective role of digital certificates.

KEYWORDS: Public Key Infrastructure, Digital Certificates, UAE Identity Management Infrastructure, E-Government

1. INTRODUCTION

Information and communications technology has demonstrated the engine capacity to transform the way businesses operate, the way that government can deliver, and the way scientific research is undertaken to improve society. In an ever-changing world, being able to respond rapidly to new opportunities and challenges is crucial to the future economic and social prosperity of the world (Greenstein, M. & Vasarhelyi, 2002; Shaw, 2006). The rapid development of Information and Communication Technologies (ICT) is forcing governments to adopt more rigorous development plans to revolutionize their operations, service delivery channels, and the way they interact with citizens.

Virtual space, electronic banking, and other electronic services are becoming more commonplace, offering the convenience and flexibility of round-the-clock service direct from the comfort of home. However, there is an increasing concern both from individuals and organizations about the privacy and security associated with electronic transactions (Germain, 2003). Encryption seems to be insufficient by itself because it provides no proof of the identity of the sender of the encrypted information. Digital certificates have emerged as a compelling technology, able to provide higher levels of security and assurances of electronic identities and content integrity.

This article provides an overview of a government program and the potential use of digital certificates. We attempt to outline the different scenarios formulated during discussions in the implementation phases of the UAE national identity management infrastructure, which was first launched in 2003. The main purpose of this article is to explore the UAE digital identity issuing authority's position with regards to G2G e-government transactions and the prospective role of digital certificates. This article is structured as follows: The first section provides a short overview of the digital certificates and their role in electronic transactions. The second section provides an overview of the UAE

Identity Authority and digital certificates. It outlines the possible scenarios of the application of government issued digital certificates, and outlines the general architecture of UAE identity infrastructure and the technical components related to digital certificates.

2. DIGITAL CERTIFICATES

Digital certificates are digital files that certify the identity of an individual or institution seeking access to computer-based information. By enabling such access, they serve the same purpose as a driver’s license or library card. Digital certificates bind the identity of an individual or institution to a digital public key, i.e., to a pair of electronic keys that can be used to encrypt and sign digital information. The combination of standards, protocols, and software that support digital certificates is called a public key infrastructure, or PKI. The software that supports this infrastructure generates sets of public-private key pairs. Public-private key pairs are codes that are related to one another through a complex mathematical algorithm. The key pairs can reside on one’s computer or on hardware devices such as smart cards or floppy disks.

Through digital certificate, it is possible to verify someone's claim that they have the right to use a given key, helping to prevent people from using phony keys, for example, to impersonate other users. Used in conjunction with encryptison, digital certificates provide a more comprehensive security solution, assuring the identity of all parties involved in a transaction.

A digital certificate is issued by a Certification Authority (CA) and signed with the CA's private key. A digital certificate typically contains the following elements: (1) owner's public key, (2) owner's name, (3) expiration date of the public key, (4) name of the issuer (the CA that issued the digital certificate), (5) serial number of the digital certificate, and (6) digital signature of the issuer.

The most commonly accepted format for digital certificates is defined by the ITU X.509[1] international standard; thus, certificates can be read or written by any application complying with X.509. Further refinements are found in the PKCS[2] standards and the PEM[3] standard.

Figure 1 depicts an example of a university campus with various methods for access control that can be integrated with a digital certificate infrastructure, e.g., Kerberos[4], passwords, and in-person ID. The diagram shows various methods

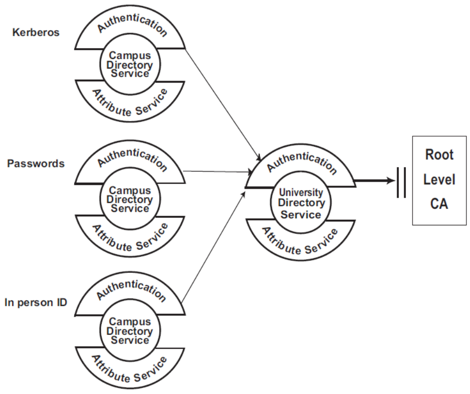
[1] **ITU X.509:** a widely used standard for defining digital certificates. X.509 (Version 1) was first issued in 1988 as a part of the ITU X.500 Directory Services standard. When X.509 was revised in 1993, two more fields were added resulting in the Version 2 format. These two additional fields support directory access control. X.509 Version 3 defines the format for certificate extensions used to store additional information regarding the certificate holder and define certificate usage. Collectively, the term X.509 refers to the latest published version, unless the version number is stated. X.509 is published as ITU recommendation ITU-T X.509 (formerly CCITT X.509) and ISO/IEC/ITU 9594-8 which defines a standard certificate format for public key certificates and certification validation. With minor differences in dates and titles, these publications provide identical text in the defining of public-key and attribute certificates.

[2] **PKCS:** is an abbreviation for Public-Key Cryptography Standards, and it refers to the set of standards for public-key cryptography, developed by RSA Laboratories in cooperation with an informal consortium, originally including Apple, Microsoft, DEC, Lotus, Sun and MIT.

[3] **PEM:** is an abbreviation for Privacy Enhanced Mail (RFC 1421 - RFC 1424), an early standard for securing electronic mail (IRTF, IETF). PEM never has been as widely adopted as Internet Mail Standard.

[4] **Kerberos** is a secure method for authenticating a request for a service in a computer network. Kerberos was developed in the Athena Project at the Massachusetts Institute of Technology (MIT). The name is taken from Greek mythology; Kerberos was a three-headed dog who guarded the gates of Hades. Kerberos lets a user request an encrypted "ticket" from

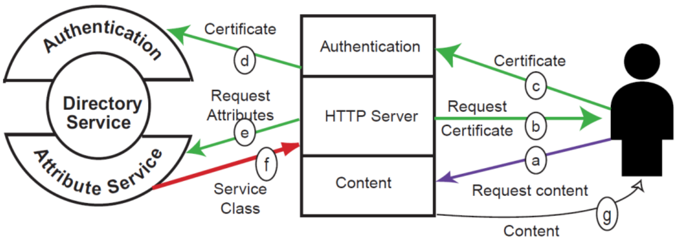
that rely on some form of directory service to authenticate a campus user for access to a service or resource. In this illustration, the University Directory Service is represented by the LDAP Authentication Database.



Source: DLF & CREN (2000)

Figure 1: Digital Certificate Application in a University Campus

Figure 2 depicts an example of the flow of information between a publisher’s server and a user’s computer using digital certificates. In this example, the client attempts access to a controlled resource from a publisher, such as a database or digital library, usually through a Web interface. The publisher’s server asks the client to present a certificate. The client presents a certificate, and the publisher’s server verifies that the certificate is authentic and authorizes access to the content.



Source: DLF & CREN (2000)

Figure 2: Digital Certificate Authentication Process

As governments continue to invest significantly in the development and deployment of e-government solutions, there is a global movement towards using digital certificates to authenticate and authorize secure interactions over virtual networks. The next section looks at the digital certificate infrastructure implementation in the United Arab Emirates.

The UAE Identity Authority

In 2003, the government of the UAE began the use of digital certificates aspect of its public key infrastructure technology deployment which was integrated with the national identity management infrastructure development program (Al-Khouri, 2011; Westland & Al-Khouri, 2010). A federal Identity Authority was established in 2004 to oversee the implementation of the program and the issuing of digital certificates in the form of smart identity cards to all members of the population. Currently more than half of the population have been registered, and the remaining five million people are

an authentication process that can then be used to request a particular service from a server. The user's password does not have to pass through the network.

expected to be enrolled by 2013. Each individual goes through a rigorous registration process where fingerprints and photos are captured at one of more than fifty registration centers in the country. The biographical data and biometrics are then processed centrally and go through automated and human validation systems which either grant or reject the issuing of identity cards.

The government is planning to achieve a strategic objective from this project: to support e-government and e-commerce initiatives. The use of public key infrastructure will enable the establishing of a secure channel for communicating any sensitive information between the different parties in an electronic environment. Generally, once a digital certificate is obtained, one may set up security-enhanced web or e-mail applications to use the digital certificate automatically.

Theoretically speaking, the use of digital certificates in e-government communications is relatively straight forward (Babaoglu, 2003). The UAE Identity Authority is in a position to issue digital certificates to government entities that want to connect to the government Identity Authority. The certificates will be used for establishing secure communications and mutual authentication between the participating parties. Extension of these services to include secure e-mail and data encryption falls outside the scope of this paper. For the moment, it is assumed that the requirement is only to use digital certificates in secure communication channels; therefore, it was recommended that the existing technical CA be used for such a purpose, which is a matter of issuing the certificates with no additional infrastructure required. The reasons for this are explained in later sections of this article.

3.1. UAE PKI Strategy Overview

As indicated earlier, there have been several discussions during the project implementation about the necessary infrastructure to extend the UAE PKI to facilitate e-services for ID card holders. There are challenges with this requirement since ID card holders will not only authenticate themselves but use digital signatures;, possibly encryption at a later stage, and they will travel around and require services from various locations. Each of these requires an extensive infrastructure which includes card readers, access to public key repository, access to the CRL repository, LDAP-accessible directory services, key escrow, etc.

For the purpose of this discussion, this paper will only focus on the need for authentication (using digital certificates) between devices in a government-to-government (or e-government) scenario.

The Political Question

Prior to getting into the technical aspects of the discussion, it is necessary to deal with some political questions in order to understand the various scenarios that might be encountered. Some questions were:

- Who will be the ultimate certificate authority issuing digital certificates in the UAE?
- Will the commercial certificate authority be the same as the government certificate authority?
- What are the roles of commercial CAs offered by the telecom companies in the country and the Identity Authority within the digital certificate space?

3.1.1 Scenario 1 – A Single CA for the UAE

Since telecom operators in the UAE run commercial CAs, they have already invested in the infrastructure and conformed to the strict requirements of hosting a trust center. The natural conclusion would be to assume that they are in the best position to provide PKI services for the government as well. This means that the UAE Identity Authority need not concern itself with any additional infrastructure regarding e-government services or ID card holder's e-services. In addition, it need not be concerned with digital certificates all together; they may act as a registration authority for the national CA, only verifying identities and approving certificates on behalf of the national CA. This, however, might not be in the best interest of national security and hence the Identity Authority.

3.1.2 Scenario 2 – Separate Commercial and Government CAs

The second scenario is that of having two separate CAs, one for commercial services and one for government services. These two CAs may autonomously function on their own and on the same level of authority. While telecom companies can perform the function of commercial CAs, the Identity Authority may perform the function of the government CA. The UAE Identity Authority is already issuing certificates for ID card holders but require the necessary infrastructure to facilitate the PKI services beyond the boundary of the national identity management infrastructure. In addition, the necessary legislation needs to be in place to have the Identity Authority function as the official government CA.

3.1.3 Scenario 3 – Hybrid CAs

The third scenario is to have the government Identity Authority provide limited PKI services in the form of ID card holder certificates and some e-government certificates, but to let the telecom companies provide integration and necessary infrastructure services. The details of such a hybrid solution are not important now, but such a solution may prove to be the best strategy for the short term. The technical discussion will resolve around the assumption that this scenario is the current way forward.

3.2. The UAE Identity Infrastructure

3.2.1 Identity System Technical CA

From the definition, a Certificate Authority (CA) is a trusted organization that maintains and issues digital certificates. The UAE Identity Authority currently has two root CAs: the Population CA and the Technical CA. The Population CA is used to issue and sign the ID card holders' certificates, which are exported to the ID cards. The Technical CA is used to issue and sign various certificates used in the national identity management system: web servers, administration tools, network appliances, fingerprint devices, etc. A few subordinate CAs exist in a hierarchy below the Technical CA: the Timestamp CA, Server CA, Admin CA, and MSO CA. The following diagram depicts a logical representation of the UAE identity management system CA design:

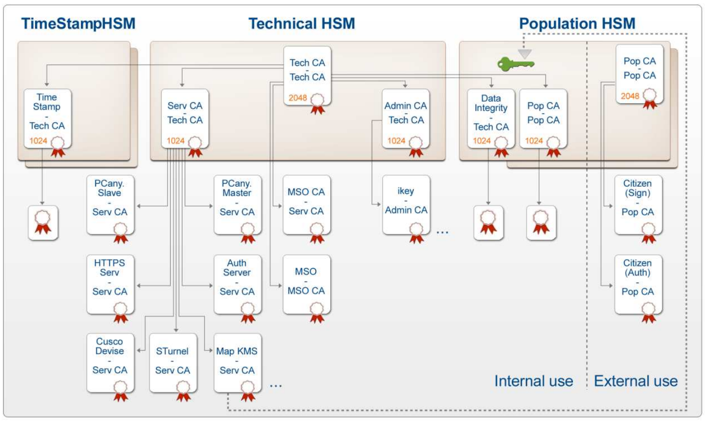


Figure 3: Logical CA Design

In order to accommodate the issuance of third-party certificates (e.g., that of other government departments), the certificates can simply be issued from one of the existing subordinate CAs, or a new subordinate CA can be created just for that purpose. In this case, it is recommended that a third-party CA be created under the Technical CA on the same level as the Server and Admin CA. The process would typically work as follows:

- A government entity wants to connect to a server in the Identity Authority DMZ.
- The connection and associated infrastructure is provided by the government entity and installed in accordance with the Identity Authority security policy.
- The government entity applies for a server (or client) certificate from the Identity Authority.
- The Identity Authority issues the certificate from the technical CA.
- The certificate gets installed in the device / client / server of the government entity.
- The connection between the government entity and the Identity Authority can now be mutually authenticated and encrypted on the upper layers of the protocol stack (i.e., SSL, SSH, etc.)
- The CRL is made available in the DMZ, so no need for further infrastructure.

This is a simplified process, but it demonstrates the use of digital certificates that are issued from the Identity Authority to authenticate and encrypt communications between the Identity Authority and other government departments. The number of such certificates will be much less than the ID card holders' certificates. Therefore the need for OCSP and a LDAP-accessible CRL is not necessary. This simplifies the solution even further.

3.2.2 Level of Trust

Validating the CA certificate is an important part of the trust associated with a PKI infrastructure (Mohapatra, 2001). The Identity Authority uses a stand-alone CA, which does not have a trusted path associated with the commercial CAs. This in itself is not a problem, but it means that the root CA certificate (public key) of the Identity Authority has to be distributed to all entities to provide CA certificate validation. This is not a problem as long as it has control over the distribution and use of the issued certificates, meaning that whenever a certificate is issued, the root CA certificate is installed with it. If, however, the certificates will be used among government entities other than the Identity

Authority, the root CA certificate must be published in a central location for everyone to access or be distributed to all government entities on a per request basis.

3.3 Certificate Uses

The scope of the e-government certificates will determine the extent of the PKI infrastructure required. The use of certificates for session authentication (e.g., SSL), as opposed to digital signatures and file encryption, allows for a much simpler infrastructure. The current infrastructure supports the use of digital certificates for this purpose within the national identity management system environment. Extending this to other government departments will be technically straight forward and will not require major changes or additions, assuming that it does not involve digital signatures and data encryption.

3.3.1 Secure Sockets Layer (SSL)

One of the best-known uses of public key encryption is the protocol known as the Secure Sockets Layer (SSL), which protects the communications channel. Every day, people access e-commerce sites to purchase goods and services over the Internet, and wish to secure their sessions with these sites to protect the confidentiality of information such as credit card numbers. The magnitude of this everyday use of SSL to protect these sites indicates that SSL is by far the most widespread commercially employed PKI technology. A typical SSL session consists of the following procedures:

- A browser sends a request to connect to a site that has a server certificate. The user performs this request by clicking on a link indicating that it leads to a secure site, or the user types in a URL with an “https” protocol specifier.
- The server responds and provides the browser with the server’s certificate.
- The browser verifies the digital signatures on the server certificate with reference to a certificate chain leading to a trusted root certificate.
- The browser also compares the server’s domain with the domain listed in the certificate to ensure that they match. If these steps are successful, the server has been authenticated to the user, providing assurances to the user that the user is accessing a real site whose identity was validated by a CA. This process is called server authentication.
- Optionally, the server may request the user’s certificate. The server can use the user’s certificate to identify the user: a process called client authentication.
- The browser generates a symmetric session key for use by the browser and server in encrypting communications between the two.
- The browser encrypts the session key with the server’s public key obtained from the server certificate and sends the encrypted key to the server.
- The server decrypts the session key using its private key.
- The browser and server use the session key to encrypt all subsequent communications.

Following these procedures, the user may notice a padlock symbol appearing on the screen. In addition, the user will be able to inspect the certificate on the site using the browser. SSL with HTTP is the only way to implement the technology. It can be used in many other services as well: SSL / LDAP; SSL / FTP; SSL / SMTP; etc. This will likely be the most used application of digital certificates in e-government implementation.

3.3.2 Secure Shell (SSH)

Secure Shell provides terminal-like access to remote computers by using a tunneling mechanism. It is especially useful in remote maintenance and troubleshooting and provides authentication and secure transmission. SSH is often used to replace Telnet, FTP, and the R-protocols in UNIX (e.g., rlogin, rexec, rsh).

3.3.3 IPSec

IPSec is used to set up a secure channel for protecting data exchange between two devices. It is currently used between sites in the national identity management system network, so it will not be explained in detail. Basically the most common implementation of IPSec is the use of symmetric key encryption rather than asymmetric (public key encryption), due to the speed advantage.

3.3.4 Secure MIME (S/MIME)

Secure MIME is a standard for encrypting and digitally signing electronic mail that contains attachments and for providing secure data transmissions. S/MIME provides confidentiality through the user’s encryption algorithm, integrity through the user’s hashing algorithm, authentication through the use of X.509 public key certificates, and non-repudiation through cryptographically signed messages. It should be noted that using S/MIME within an e-government scenario will require extension of the PKI infrastructure, especially when e-mail encryption is used.

4. CONCLUSIONS

This article has presented an overview of various scenarios of the usage and application of digital certificates in the United Arab Emirates. For the short term, the UAE Identity Authority can extend its technical CA services to third-party government entities with little effort, depending on the scope and configuration of the requirement. For the long term, it needs to position itself strategically. It will be vital to have a roadmap for PKI services in the UAE (the government specifically) and the role of the UAE Identity Authority, in addition to its relationship with telecom operators.

5. REFERENCES

1. Al-Khouri, A. M. (2011) "PKI in Government Identity Management Systems", International Journal of Network Security & Its Applications, vol.3, No.3, pp. 69-96.

2. Babaoglu, O. (2003) Certificates, Certification Authorities and Public Key Infrastructures [Online]. http://www.cs.unibo.it/babaoglu/courses/security/lucidi/PKI.pdf, Accessed [10 October, 2011].

3. DLF & CREN (2000) Digital Certificate Infrastructure: FAQ, Digital Library Federation & Corporation for Research and Educational Networking, http://www.diglib.org/architectures/cren-dlf.pdf Accessed [10 October, 2011].

4. Germain, J.M. (2003) Beyond Biometrics: New strategies for security, E-Commerce Times [Online]. http://www.ecommercetimes.com/perl/story/ 31547.html Accessed [10 October, 2011].

5. Greenstein, M. and Vasarhelyi, M. (2002) Electronic Commerce: Security, Risk Management and Control, McGraw-Hill, New York.

6. Mohapatra, P.K. (2001) Public Key Cryptography, ACM Crossroads Student Magazine [Online]. http://www.acm.org/crossroads/xrds7-1/crypto.html Accessed [10 October, 2011].

7. Shaw, M.J. (Ed.) (2006) E-Commerce and the Digital Economy. M E Sharpe Inc.

8. Westland, D. & Al-Khouri, A.M. (2010) "Supporting e-Government Progress in the United Arab Emirates", Journal of E-Government Studies and Best Practices, vol. 2010. pp.1-9.